

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

(12) UK Patent Application (19) GB (11) 2 350 982 (13) A

(43) Date of A Publication 13.12.2000

(21) Application No 9913530.3

(22) Date of Filing 10.06.1999

(71) Applicant(s)

John Quentin Phillipps
30 Mount Avenue, Ealing, LONDON, W5 2QJ,
United Kingdom

(72) Inventor(s)

John Quentin Phillipps

(74) Agent and/or Address for Service

Venner Shipley & Co
20 Little Britain, LONDON, EC1A 7DH,
United Kingdom

(51) INT CL⁷

G06F 17/60 , G07F 7/10 , H04L 12/22

(52) UK CL (Edition R)

H4P PPEB

(56) Documents Cited

EP 0813325 A2 EP 0590861 A2 EP 0501697 A2

(58) Field of Search

UK CL (Edition R) H4P PDCSA PPEB
INT CL⁷ G06F 1/00 17/60 , G07F 7/08 7/10 , H04L
12/22 29/06
Online: EPODOC, JAPIO, WPI

(54) Abstract Title

Electronic commerce system where credit card details are not transmitted over insecure networks

(57) Users 101-103 access vendors 107,108 via the PSTN 104, internet service provider (ISP) 109 and the internet 106. The vendors are registered with the ISP so that when a user makes a purchase the ISP recognises and intercepts the Action URL of the vendors credit card details submission form. The ISP sends the form to the transaction computer 112 of a financial services provider over a leased line 115.

The transaction computer checks the form and replies with a 'not approved' message or an 'approved' message including a transaction ID. The ISP then either forwards the 'not approved' message or replaces the credit card details in the credit card details submission form with the transaction ID and forwards the modified form to the vendor. The transaction ID is then submitted to the financial service provider along with the request for payment, and validated against the financial service providers records before payment is authorised.

Thus the credit or debit card details are only transmitted over the relatively secure PSTN links 4 and the leased line 115. The financial services and internet service providers may alternatively constitute a single entity (see Fig. 1).

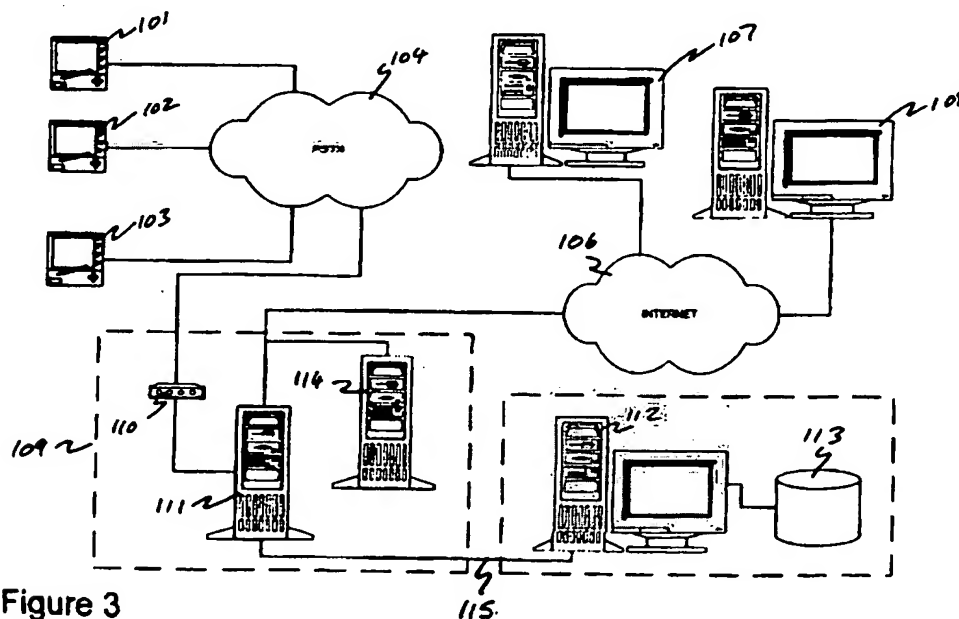


Figure 3

GB 2 350 982 A

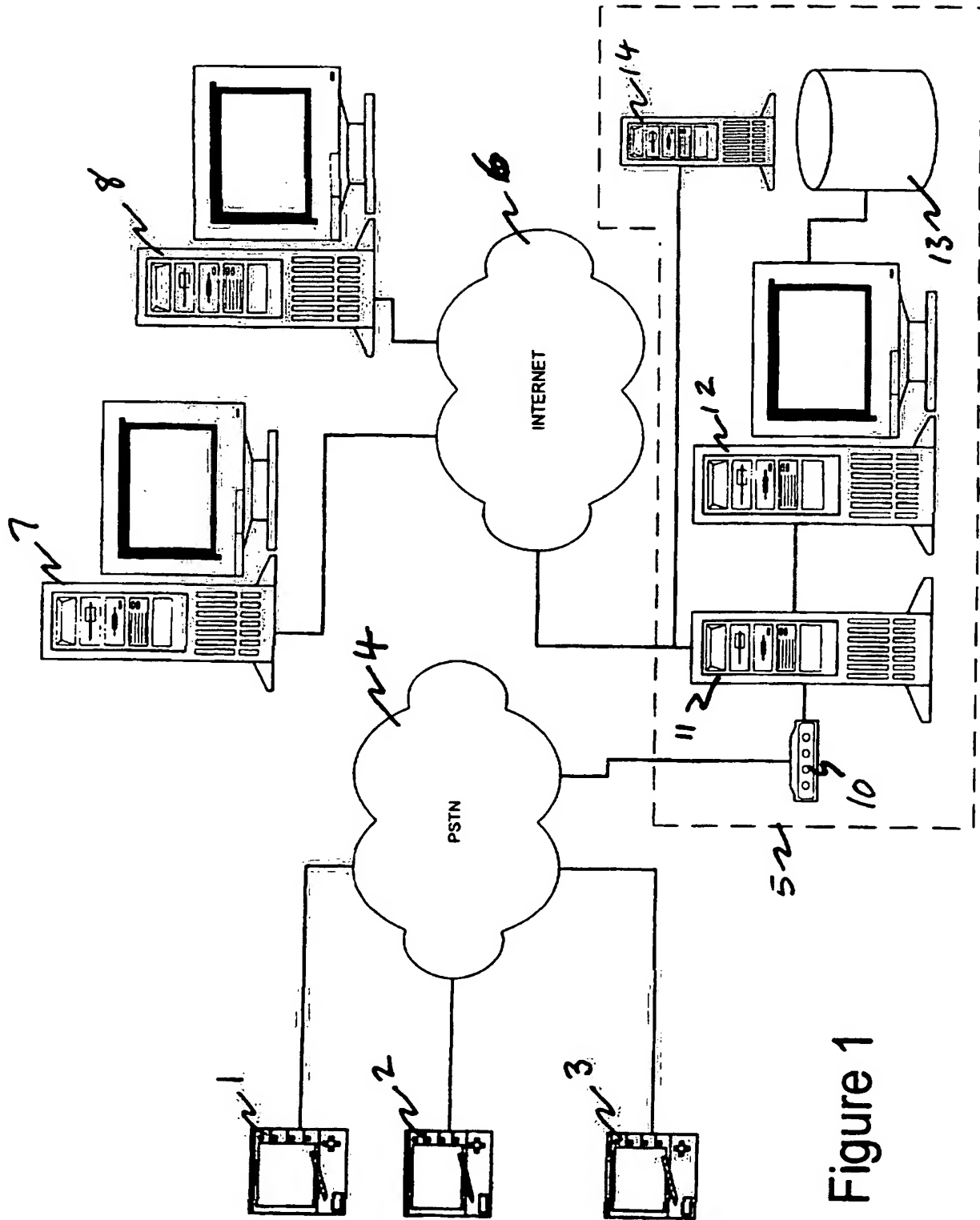


Figure 1

—

Web Browser

×

File Edit View Go Bookmarks Options Directory Window Help

URL <http://www.examplevendor.co.uk/orders/creditcardform.html>

Credit Card Details

Mastercard

☒

Visa

☐

Number

Expiry

05

1999

Name

Street

City

Postcode/Zip

Country

Submit

Clear

Figure 2

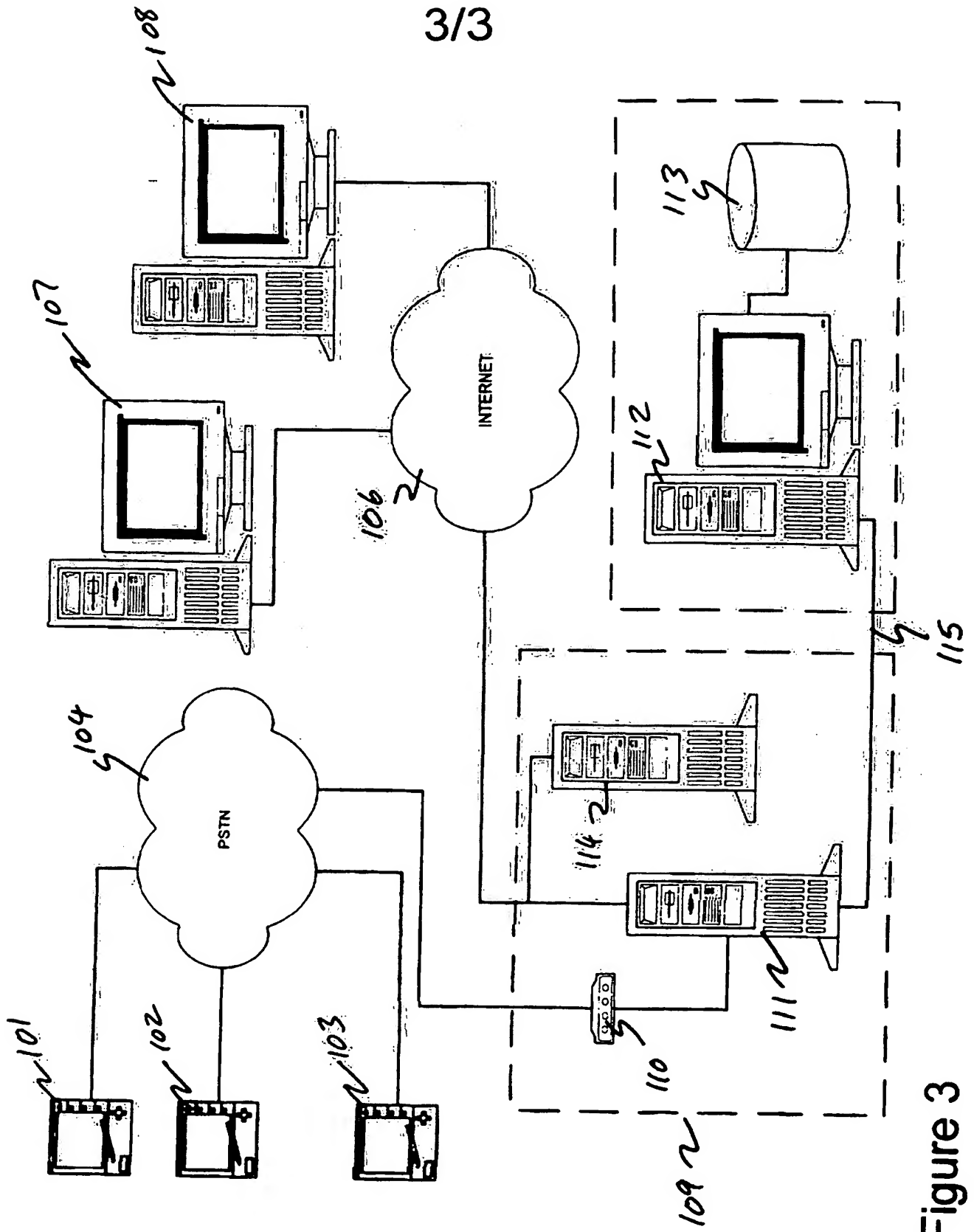


Figure 3

Electronic Commerce System

Description

The present invention relates to an electronic commerce system.

5

Internet commerce is a rapidly expanding area. Many goods and services can be ordered via the Internet. To do this, a user typically uses a web browser, such as Netscape Navigator or Microsoft Internet Explorer, to visit a web site of a vendor. The web site will include pages enabling the user to select the goods or services required and a page containing a form by means of which the user can enter their credit or debit card details so that the vendor can receive payment for the ordered goods or services.

10

A disadvantage of this arrangement is that the user must send their credit or debit card details to the vendor via the Internet. The Internet is not a fully secure network and there is the possibility that the credit or debit card details may be intercepted and used in the perpetration of a fraud.

15

It is an aim of the present invention to provide for Internet commerce whilst avoiding the transmission of credit or debit card details via the Internet itself.

20

According to the present invention, there is provided an electronic commerce system comprising an Internet connectivity provider site, a financial service provider site for producing transaction IDs, a user terminal programmed with a web browser program and connectable to the Internet connectivity provider site for accessing the Internet, and a World Wide Web vendor site configured for sending a payment card information entry form, e.g. an HTML form, having an action definition, e.g. an action URL, having at least one parameter, associated therewith, wherein the Internet connectivity provider site is configured to intercept messages from the user terminal which include said action definition and substitute at least a payment card number (e.g. credit card or debit card number) within the parameter or parameters of said action definition with a transaction ID produced by the financial service provider site. It should be noted that since the Internet connectivity provider site is providing connectivity to the Internet for the user terminal, the

25

30

user terminal will not therefore be communicating with the Internet connectivity provider site via the Internet.

5 Thus in a system according to the present invention, payment card numbers are stripped from messages before the messages enter the Internet. Furthermore, the vendor site can still be used by customers, accessing the World Wide Web by means other than the Internet connectivity provider site, and requires minimal modification from a typical vendor site configuration.

10 A user terminal for a system according to the present invention preferably comprises a computer including user input means, modem means and modem control data for controlling the modem for establishing communication with the Internet connectivity provider site, wherein the modem control data is not modifiable by means of data input using the user input means alone. More preferably, the user terminal includes read-only
15 storage means storing an machine-specific ID. This ID can be used to confirm the identity of a person sending payment card details from the user terminal.

A World Wide Web vendor site for a system according to the present invention is preferably configured to run a process for processing said action definition, said process
20 being capable of:-

recognising unsubstituted parameters and recording a transaction in a first manner in response thereto; and

recognising substituted parameters, which identify a transaction, and recording the transaction in a second manner in response thereto.

25 More preferably, said process is capable of recognising substituted parameters which indicate a reason (e.g. insufficient credit or incorrectly entered payment card related data) for non-completion of the transaction and sending a page to the user terminal in dependence thereon.

30 An Internet connectivity provider site for a system according to the present invention preferably includes:-

a database of vendor site IP addresses and associated action definitions;

search means for searching the database for the destination IP address in a message from the user terminal;

identification means responsive to the search means finding an IP address in the database to identify said action definition in the message; and

5 signalling means for signalling action definition parameters to the financial service provider site in dependence on identification of an action definition by the identification means and receiving a transaction ID or other data not comprising a payment card number therefrom;

means for substituting at least a payment card number within the parameter or
10 parameters of said action definition with the transaction ID or other data; and

transmission means for sending the modified message to the vendor site.

Preferably, the transmission means is configured to mimic the user terminal when sending said modified message.

15

The Internet connecting provider site may be integrated with the financial service provider site.

Embodiments of the present invention will now be described, by way of example,
20 with reference to the accompanying drawings, in which:-

Figure 1 shows the hardware of first, second and third embodiment of the present invention;

Figure 2 shows an exemplary credit card details entry HTML form; and

Figure 3 shows the hardware of a fourth embodiment of the present invention;

25

Referring to Figure 1, first, second and third user terminals 1, 2, 3 are connectable via the pstn (public switched telephone network) 4 to a financial service provider site 5. The financial service provider site 5 is connectable via the Internet 6 to first and second Internet vendor sites 7, 8. The number of user terminals 1, 2, 3 is not
30 restricted to three. Similarly, there may be many more Internet vendor sites than the two Internet vendor sites 6, 7 shown.

The first user terminal 1 comprises a pad-type computer, such as the Cyrix® WebPAD™, which includes a modem. WindowsCE is used as the operating system for the first user terminal 1. However, the dial-up networking configuration user interface is disabled so that a user cannot alter the Internet connectivity provider used for Internet access. A web browser program is provided on the first user terminal 1 so that the user can access the World Wide Web using the terminal's modem.

The second and third user terminals 2, 3 are of the same construction as the first user terminal 1.

The vendor sites 7, 8 comprise web servers. The vendor sites 7, 8 provide HTML forms (Figure 2) that enable a user to enter their credit card number and expiry date and their address.

The financial service provider site 5 comprises a modem bank 10 connected between the pstn 4 and a communication computer 11. The communication computer 11 is also connected to the Internet 6 and to a transaction processor comprising a transaction computer 12 and a database 13. The financial service provider site 5 also comprises a domain name server (DNS) 14. The financial service provider site 5 is thus configured for the financial service provider to provide Internet connectivity to the user terminals 1, 2, 3.

All datagrams to be sent via the Internet 6 from user terminals 1, 2, 3 pass through the communication computer 11. The communication computer 11 contains a database of registered vendor sites 7, 8 including their IP addresses and the "action" URL of the vendor's credit card details form.

The making of a purchase by the user of user terminal 1 from the first Internet vendor site 7 will now be described. It will be appreciated that the method is effected by a conventional web browser running on the first user terminal 1 and custom programs running on the communication computer 11, the transaction computer 12 and the web server at the first vendor site 7.

The user of the first user terminal 1 switches on the first user terminal 1 and runs the web browser program. This causes the first user terminal 1 to dial up the financial service provider site 5 and log on as with any Internet connectivity provider
5 providing dial-up Internet access. The web browser will submit an initial URL, e.g. for a search engine such as Yahoo or Alta Vista, or the home page of the financial service provider.

10 A name resolver process running on the first user terminal sends the server part of the URL to the DNS 14 and receives back the IP address of that server. The URL is then sent from the first user terminal 1 in a message to the returned IP address.

The datagrams from the first user terminal are received by the communication machine 11. The communication machine 11 reads the destination IP address in the
15 header of the first datagram or a message and looks it up in its database of registered vendor sites. Since, in this case, the IP address is not for a registered vendor site, the first datagram is forwarded immediately to the Internet 6 and the subsequent datagrams of the message are forwarded as soon as possible to the Internet 6. In this case the communication computer 111 now operates merely as a
20 router for subsequent datagrams of the message.

The destination server responds to the URL in the message from the first user terminal 1 by replying with a message containing HTML code for a page. The datagrams of this message are routed by the Internet 6 to the communication
25 computer 11 which then routes them via the modem bank 10 along the pstn connection to the first user terminal 1. The web browser, running on the first user terminal 1, then displays the page defined by the HTML in the reply message.

30 The system operates in this manner until, the first user terminal 1 sends a URL addressed to, for example, the first vendor site 7 which, for example, identifies the vendor's home page. In this case, the communication computer 11 finds the destination IP address in the first datagram of the message containing the URL in its database. Thus, rather than immediately forwarding the datagrams of the message,

the communication computer 11 caches the datagrams until the whole message has been received. When the whole message has been received, the communication machine 11 analyses the message to determine whether it contains the "action" URL of the destination vendor's credit card details form as contained in its database.

5 Since, the URL is for the vendor's home page, the datagrams are now forwarded unmodified to the first vendor site 7 via the Internet 7.

At the TCP level, once the communication computer 11 has identified that a datagram from the first user terminal 1 is addressed to the first vendor site 7, it
10 must respond to the first user terminal 1 as if it were the first vendor site 7 for connection set up, data transfer and connection termination. Also, when the communication computer 11 forwards the cached message to the first vendor site 7, it must mimic the first user terminal 1 so that the response to the sent URL is correctly addressed to the first user terminal 1 and lost or corrupted datagrams are
15 retransmitted.

It will now be assumed that the user of the first user terminal 1 has decided to make a purchase and has received the first vendor's credit card details form. The user fills in the form and clicks on the SUBMIT button (see Figure 2). This causes the
20 form's action URL to be submitted. The message containing the action URL is intercepted by the communication machine 11 as described above. However, the communication computer 11 now determines that the action URL is present.

On determining that the action URL is present, the communication computer 11
25 sends the action URL to the transaction computer 12. The transaction computer 12 compares the data in the action URL with card holder details in the database 13. If the data is incorrect, e.g. the address is not that of the card holder, the transaction computer 12 sends back the message "invalid" to the communication computer 11. The communication computer 11 then strips the data from the action URL and
30 replaced it with the name-value pair "details=invalid". The reconstructed action URL is then sent to the first vendor site 7 with the communication computer 11 mimicking the first user terminal 1.

It will be appreciated that a standard action URL used by all vendors would simplify the extraction of the card and user details from the action URL.

5 The process at the first vendor site 7, which handles the action URL, identifies the "details=invalid" name-value pair and sends an error warning HTML page to the first user terminal 1. This page is then displayed by the web browser running on the first user terminal 1.

10 If the data in the action URL is correct, the transaction computer 12 generates a unique transaction ID, which it stores in the database 13 against the card holder's account, and sends the transaction ID to the communication computer 11. The communication computer 11 then strips the data from the action URL and replaced it with the name-value pair "ID=nnnnnnnn" where n is a character of the transaction ID. The reconstructed action URL is then sent to the first vendor site 7
15 with the communication computer 11 mimicking the first user terminal 1.

On receiving the modified action URL, the action URL-handling process of the first vendor site 7 validates and logs the transaction ID for later confirmation of the transaction with the credit card company and sends a confirmation HTML page to
20 the first user terminal 1.

Logged transaction IDs are sent by a secure means, e.g. a direct psdn connection, to the credit card company together with the amount to be charged. The credit card company then compares the transaction ID with the records in the database 13
25 before authorising the transfer of funds to the first vendor.

In a second embodiment having the hardware configuration shown in Figure 1, the action URL produced by the credit card form (Figure 2) includes the value of the transaction. This information is sent by the communication computer 11 to the
30 transaction computer 12 with the credit card number and card holder details. The transaction computer 12 then determines by reference to the database 13 whether the user has sufficient credit for the transaction. If the user does not have sufficient credit for the transaction, the transaction computer 12 sends the message

“insufficient credit” to the communication computer 11. The communication computer 11 then strips the data from the action URL and replaced it with the name-value pair “details=insufficient credit”. The reconstructed action URL is then sent to the first vendor site 7 with the communication computer 11 mimicking the first user terminal 1.

The process at the first vendor site 7, which handles the action URL, identifies the “details=insufficient credit” name-value pair and sends an error warning HTML page to the first user terminal 1. This page is then displayed by the web browser running on the first user terminal 1.

In a third embodiment having the hardware configuration shown in Figure 1, the user terminals 1, 2, 3 are provided with unique IDs, e.g. chip-specific IDs for their processors. In this case, the operation of the communication computer 11 is modified so that on receipt of an action URL for a registerer vendor site 6, 7, it sends a message to the user terminal 1, 2, 3 requesting the ID. A process running on the user terminal 1, 2, 3 responds to this message by sending the ID back to the communication computer 11. If the ID is not received by the communication machine within a predetermined time the connection to the user terminal 1, 2, 3 is dropped as it is assumed that the user terminal 1, 2, 3 is not an authorised terminal.

If an ID is received, it is passed to the transaction computer 12 with the data from the action URL. The transaction computer 12 tries to match the ID with the credit card number. If there is a match, the process proceeds as in the first embodiment. However, if there is not a match, the transaction computer 12 sends the message “imposter” to the communication computer 11 which responds by dropping the connection to the user terminal 1, 2, 3.

In either exception condition, caller line identification (CLI) can be used to identify the telephone line used to dial into the financial service provider site 5. This number can then be passed to a law-enforcement agency with a report of an attempted credit card fraud.

Referring to Figure 3, first, second and third user terminals 101, 102, 103 are connectable via the pstn (public switched telephone network) 104 to an Internet connectivity provider site 109. A financial service provider site 105 is connected to the Internet connectivity provider site 109 by a leased line 115. Internet

connectivity provider site 109 is connectable via the Internet 106 to first and second Internet vendor sites 107, 108. The number of user terminals 101, 102, 103 is not restricted to three. Similarly, there may be many more Internet vendor sites than the two Internet vendor sites 106, 107 shown.

The first user terminal 101 comprises a pad-type computer, such as the Cyrix® WebPAD™, which includes a modem. WindowsCE is used as the operating system for the first user terminal 101. However, the dial-up networking configuration user interface is disabled so that a user cannot alter the Internet connectivity provider used for Internet access. A web browser program is provided on the first user terminal 101 so that the user can access the World Wide Web using the terminal's modem.

The second and third user terminals 102, 103 are of the same construction as the first user terminal 101.

The vendor sites 107, 108 comprise web servers. The vendor sites 107, 108 provide HTML forms (Figure 2) that enable a user to enter their credit card number and expiry date and their address.

The Internet connectivity provider site 109 comprises a modem bank 110 connected between the pstn 104 and a communication computer 111. The communication computer 111 is also connected to the Internet 106. The Internet connectivity provider site 109 also comprises a domain name server (DNS) 114.

The financial service provider site 105 comprises a transaction computer 112 and a database 113. The transaction computer 112 is connected to the communication computer 111 by the leased line 115.

All datagrams to be sent via the Internet 106 from user terminals 101, 102, 103 pass through the communication computer 111. The communication computer 111 contains a database of registered vendor sites 107, 108 including their IP addresses and the "action" URL of the vendor's credit card details form.

5

The making of a purchase by the user of user terminal 101 from the first Internet vendor site 107 will now be described. It will be appreciated that the method is effected by a conventional web browser running on the first user terminal 101 and custom programs running on the communication computer 111, the transaction
10 computer 112 and the web server at the first vendor site 107.

The user of the first user terminal 101 switches on the first user terminal 101 and runs the web browser program. This causes the first user terminal 101 to dial up the Internet connectivity provider site 109 and log on as with any Internet
15 connectivity provider providing dial-up Internet access. The web browser will submit an initial URL, e.g. for a search engine such as Yahoo or Alta Vista, or the home page of the Internet connectivity service provider.

A name resolver process running on the first user terminal sends the server part of
20 the URL to the DNS 114 and receives back the IP address of that server. The URL is then sent from the first user terminal 101 in a message to the returned IP address.

The datagrams from the first user terminal 101 are received by the communication machine 111. The communication machine 111 reads the destination IP address in
25 the header of the first datagram and looks it up in its database of registered vendor sites. Since, in this case, the IP address is not for a registered vendor site 107, 108, the first datagram is forwarded immediately to the Internet 106 and the subsequent datagrams of the message are also immediately forwarded to the Internet 106. In this case the communication computer 111 now operates merely as a router for
30 subsequent datagrams of the message.

The destination server responds to the URL in the message from the first user terminal 101 by replying with a message containing HTML code for a page. The

datagrams of this message are routed by the Internet 106 to the communication computer 111 which then routes them via the modem bank 110 along the pstn connection to the first user terminal 101. The web browser, running on the first user terminal 101, then displays the page defined by the HTML in the reply message.

The system operates in this manner until, the first user terminal 101 sends a URL addressed to the first vendor site 107 which, for example, identifies the vendor's home page. In this case, the communication computer 11 finds the destination IP address in the first datagram of the message containing the URL in its database. Thus rather than immediately forwarding the datagrams of the message, the communication computer 111 caches the datagrams until the whole message has been received. When the whole message has been received, the communication machine 111 analyses the message to determine whether it contains the "action" URL of the destination vendor's credit card details form as contained in its database. Since, the URL is for the vendor's home page, the datagrams are now forwarded unmodified to the first vendor site 107 via the Internet 106.

At the TCP level, once the communication computer 111 has identified that a datagram from the first user terminal 101 is addressed to the first vendor site 107, it must respond to the first user terminal 101 as if it were the first vendor site 107 for connection set up, data transfer and connection termination. Also, when the communication computer 111 forwards the cached message to the first vendor site 107, it must mimic the first user terminal 101 so that the response to the sent URL is correctly addressed to the first user terminal 101 and lost or corrupted datagrams are retransmitted.

It will now be assumed that the user of the first user terminal 101 has decided to make a purchase and has received the first vendor's credit card details form (Figure 2). The user fills in the form and clicks on the SUBMIT button (Figure 2). This causes the form's action URL to be submitted. The message containing the action URL is intercepted by the communication machine 111 as described above.

However, the communication computer 111 now determines that the action URL is present.

On determining that the action URL is present, the communication computer 111
5 sends the action URL to the transaction computer 112. The transaction computer
112 compares the data in the action URL with card holder details in the database
113. If the data is incorrect, e.g. the address is not that of the card holder, the
transaction computer 112 sends back the message "invalid" to the communication
computer 111. The communication computer 111 then strips the data from the
10 action URL and replaced it with the name-value pair "details=invalid". The
reconstructed action URL is then sent to the first vendor site 107 with the
communication computer 111 mimicking the first user terminal 101.

The process at the first vendor site 107, which handles the action URL, identifies
15 the "details=invalid" name-value pair and sends an error warning HTML page to
the first user terminal 101. This page is then displayed by the web browser running
on the first user terminal 101.

If the data in the action URL is correct, the transaction computer 112 generates a
20 unique transaction ID, which it stores in the database 113 against the card holder's
account, and sends the transaction ID to the communication computer 111. The
communication computer 111 then strips the data from the action URL and
replaced it with the name-value pair "ID=nnnnnnnn" where n is a character of the
transaction ID. The reconstructed action URL is then sent to the first vendor site
25 107 with the communication computer 111 mimicking the first user terminal 101.

On receiving the modified action URL, the action URL-handling process of the first
vendor site 107 validates and logs the transaction ID for later confirmation of the
transaction with the credit card company and sends a confirmation HTML page to
30 the first user terminal 101.

Logged transaction IDs are send by a secure means, e.g. a direct pstn connection, to
the credit card company together with the amount to be charged. The credit card

company then compares the transaction ID with the records in the database 113 before authorising the transfer of funds to the first vendor.

5 In each of the foregoing embodiments, a user cannot change the dial-up networking setup of their user terminal 1, 2, 3. However, changing circumstances may make a change necessary, e.g. changes in the telephone number to be dialled. These changes can be made by means of a JAVA™ or ActiveX applet associated with a web page provided by the Internet connectivity providing entity.

10 The operation of the communication computer 11, 111 in any of the foregoing embodiments may be modified so that all messages from the user terminals 1, 2, 3, 101, 102, 103 are cached. The communication computer 11, 111 can then analyse the content of the messages to determine whether is comprises an action URL of a credit card details form of an unregistered "vendor". These messages can then be
15 blocked to avoid credit card details being sent to bogus vendors.

The connection between the user terminals 1, 2, 3, 101, 102, 103 and the communication computer 11, 111 may be, but not exclusively so, via a telephone circuit, on ISDN connection or a leased line.

20

It will be appreciated that many modifications can be made to the above-described embodiments to provide security beyond that obtained by avoiding the transmission of credit card details over the Internet.

25 The present invention has been explained with reference to a system employing HTML. However, it will be appreciated that with the development of XML, other mark up languages may be developed that are useable in embodiments of the present invention.

Claims

1. An electronic commerce system comprising:-
an Internet connectivity provider site;
5 a financial service provider site for producing transaction IDs;
a user terminal programmed with a web browser program and connectable to the
Internet connectivity provider site for accessing the Internet; and
a World Wide Web vendor site configured for sending a payment card information
entry form having an action definition, having at least one parameter, associated therewith,
10 wherein the Internet connectivity provider site is configured to intercept messages from the
user terminal which include said action definition and substitute at least a payment card
number within the parameter or parameters of said action definition with a transaction ID
produced by the financial service provider site.
- 15 2. A system according to claim 1, wherein said entry form is an HTML form and said
action definition comprises an action URL defined in the HTML code for said form.
3. A user terminal for a system according to claim 1 or 2, comprising a computer
including user input means, modem means and modem control data for controlling the
20 modem for establishing communication with the Internet connectivity provider site,
wherein the modem control data is not modifiable by means of data input using the user
input means alone.
4. A user terminal according to claim 3, including read-only storage means storing an
25 machine-specific ID.
5. A World Wide Web vendor site for a system according to claim 1 or 2, configured
to run a process for processing said action definition, said process being capable of:-
recognising unsubstituted parameters and recording a transaction in a first manner
30 in response thereto; and
recognising substituted parameters, which identify a transaction, and recording the
transaction in a second manner in response thereto.

6. A World Wide Web vendor site according to claim 5, wherein said process is capable of recognising substituted parameters which indicate a reason for non-completion of the transaction and sending an page to the user terminal in dependence thereon.

5 7. A World Wide Web vendor site according to claim 5, wherein said reason is insufficient credit or incorrectly entered payment card related data.

8. An Internet connectivity provider site for a system according to claim 1 or 2, including:-

10 a database of vendor site IP addresses and associated action definitions;
search means for searching the database for the destination IP address in a message from the user terminal;

identification means responsive to the search means finding an IP address in the database to identify said action definition in the message; and

15 signalling means for signalling action definition parameters to the financial service provider site in dependence on identification of an action definition by the identification means and receiving a transaction ID or other data not comprising a payment card number therefrom;

means for substituting at least a payment card number within the parameter or
20 parameters of said action definition with the transaction ID or other data; and

transmission means for sending the modified message to the vendor site.

9. An Internet connectivity provider site according to claim 8, wherein the transmission means is configured to mimic the user terminal when sending said modified
25 message.

10. An electronic commerce system substantially as hereinbefore described with reference to Figures 1 or 3.